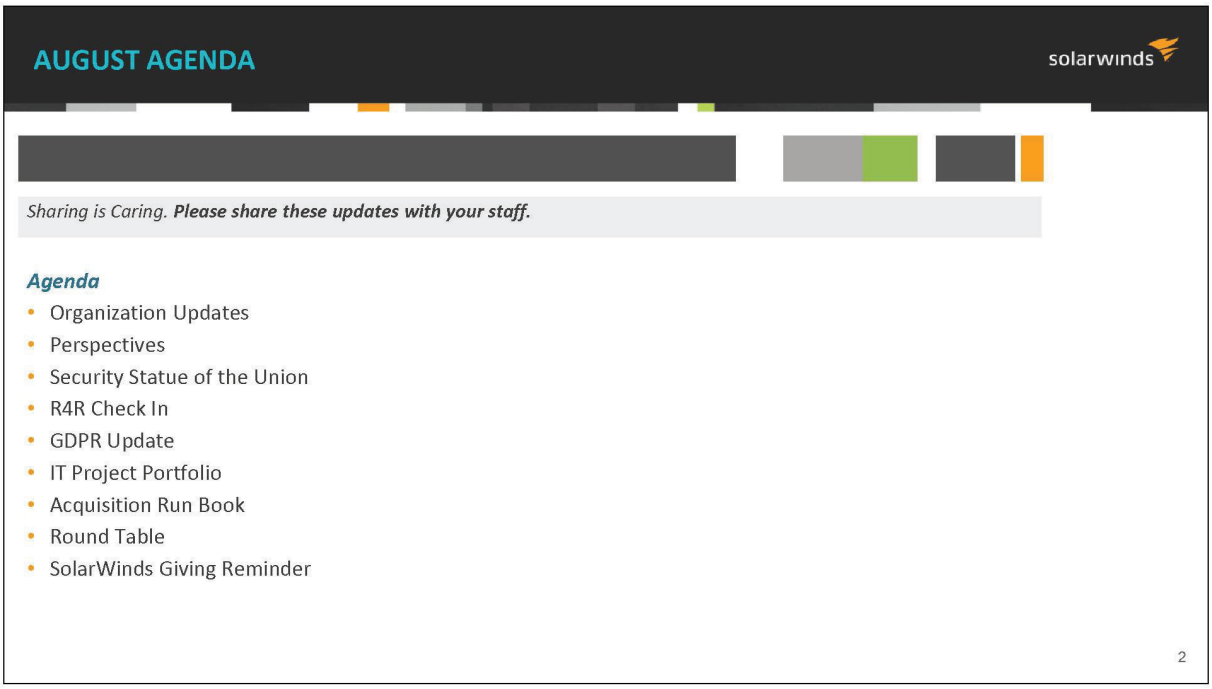
EXHIBIT 7

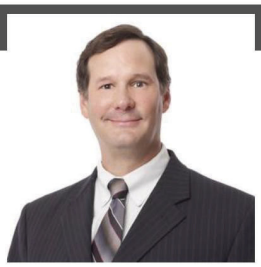

solarwinds
MONTHLY IT LEADERSHIP MEETING
CONFIDENTIAL
DEVELOPMENT OPERATIONS & INFORMATION TECHNOLOGY (DOIT)


AUGUST AGENDA
solarwinds
Sharing is Caring. Please share these updates with your staff.
Agenda
Organization Updates
Perspectives
Security Statue of the Union
R4R Check In
GDPR Update
IT Project Portfolio
Acquisition Run Book
Round Table
SolarWinds Giving Reminder
2

BUSINESS OUTLOOK

Security State of the Union

solarwinds



5

A PROACTIVE SECURITY MODEL

- $660K INVESTMENT REQUEST. ACCELERATION OPPORTUNITY

solarwinds

Risk Mitigation Plan for IT Security Operations

1. **Lock down our critical assets that could cause a major event**
   - *External **PEN test** of our environment – Provide a baseline*
   - *Lock down administrative **access** and improve **identity management** process and procedures*
   - *Implement **Web Application FW** to protect our critical web properties*
2. **Improve Cyber Hygiene so we are not a target of opportunity**
   - *Improve coverage for **endpoint security, encryption, event management***
   - *Improve system **scanning** coverage, monitoring and patching and implement DLP*
   - *Implement **security training** for all employee's*
3. **Focus on security areas that provide the biggest impact**
   - *Coordinate IT Security Ops activities across all organizations. **Standardize** policies, share best practices and coordinate the **measurement of risk** for the organization*
   - *Create legal approved **security questionnaire** answers*
   - ***Reduce the number of security incidents** by implementing industry standard best practices.*
   - *Accelerate **cross company adoption of all security controls***

Risk Mitigation Plan for Product Security / Dev Ops

1. **Establish a global, cross-pillar Security Champions – Product team members**
   - *Dotted line reporting to VP Security Arch. 30% time dedicated to security.*
   - *Internal Training and Outreach*
   - *Coordinate internal product security testing and application vulnerability scanning*
   - *Internal bug bounty program*
   - *Product Management and Engineering management coordination*
   - *Measurement of risk and effectiveness of program per product line*
2. **Invest in Commercial code scanning tool**
3. **Invest in developer security training**

A PROACTIVE SECURITY MODEL

- $660K INVESTMENT REQUEST. ACCELERATION OPPORTUNITY

solarwinds

Budget Request

Description	Annual $
Security Program Manager	$180
Security Analyst	$180
Application Firewall	$40
Internal/External PEN test	$100
Security Training	$30
Secure Development Training	$30
Commercial application code scanners	$100
Total	**$660**

Risk of Non-Investment

- Current state of security leaves us in a very ***vulnerable state*** for our critical assets. A compromise of these assets would ***damage our reputation and impact us financially***.
- Lack of cyber hygiene leaves us ***open to being a target*** of opportunity and a compromise will create downtime and lost revenue
- We have had ***28 logged security incidents*** this year to date. Reactive responses costs significantly more than being proactive.
- We have ***lost a renewal*** of DPA for Accenture (192K) due to utilizing free code scanning tools that did not find all vulnerabilities.
- Without training our **employees** will continue to be one of our ***biggest risks***
- Appropriate security policies, procedures, training, PEN testing are required by our commercial customers and asked for in ***qualifying questionnaires***. Without appropriate answers we will lose business

7